Dr.-Ing. Mario Heiderich, Cure53
Wilmersdorfer Str. 106
D 10629 Berlin
cure53.de · mario@cure53.de

Independent Security Audit of the Tangem Mobile Wallet Cryptography, SDK, and Application Security Reviewed by Cure53 (Q4 2025)

Cure53, Dr.-Ing. M. Heiderich, Dr. D. Bleichenbacher, Dr. N. Kobeissi, BSc. N. Aubry, J. de Hen, Dipl.-Ing. D. Gstir

Cure53, a Berlin-based IT security consulting firm, was engaged to conduct a penetration test, source code audit, and cryptography review of the Tangem Android and iOS SDKs, as completed in Q4 2025.

For background information, management officials from Tangem AG specified the scope and aims during preliminary conversations held in September 2025. Cure53 carried out the security-focused undertakings in November 2025 (across CW45 and CW46). Twenty-three days were designated by the client to glean an accurate estimation of the targets.

The project comprised four unique work packages (WPs) highlighting each key area of interest. These were defined as follows:

- **WP1**: White-box security tests & code audits against Tangem Android SDK
- **WP2**: White-box security tests & code audits against Tangem iOS SDK
- **WP3**: White-box cryptography audits & reviews against Tangem Android SDK
- **WP4**: White-box cryptography audits & reviews against Tangem iOS SDK

Six senior testers from Cure53 were assigned to handle the preparation, execution, and finalization of the project. A white-box methodology was used, with the internal teams providing source code, application builds, and technical documentation. All preparations were completed in the week prior to the active review (CW44) to resolve setup issues and ensure the testing phase started without delays.

Communication was handled via a dedicated Slack channel restricted to active personnel from both companies. This forum was used for all discussions, asset transfers, and technical coordination, which prevented blockers or delays. Although live reporting was not required for this project, the testing team provided frequent status updates to keep the development team informed of progress.

The assessment provided thorough coverage of the WP1-WP4 scope, identifying twelve findings. Tangem successfully remediated all findings that posed a measurable risk to security (three vulnerabilities) along with seven less significant findings. The remaining two items were confirmed as low-impact weaknesses with negligible exploitation potential. The fixes were reviewed and validated by Cure53, confirming that the WP1-WP4 scope fully meets the security requirements necessary for a secure production state.

The consistency found in both the iOS and Android app variants shows a clear focus on platform-native security. It is a solid result, yet Cure53 advises against complacency as the SDK grows. Establishing a cadence for periodic security assessments will be vital to verify that new features maintain this proficiency and that the platform remains resilient against an evolving threat landscape.

Overall, the security posture of the Tangem Mobile SDK is strong, supported by fundamental controls and a well-designed architecture. This is evidenced by the results of the assessment, which identified no vulnerabilities at the Critical or High-severity levels. Nevertheless, the assessment revealed various flaws that, while not presenting an immediate exploitation risk, offer clear paths for structural improvement.